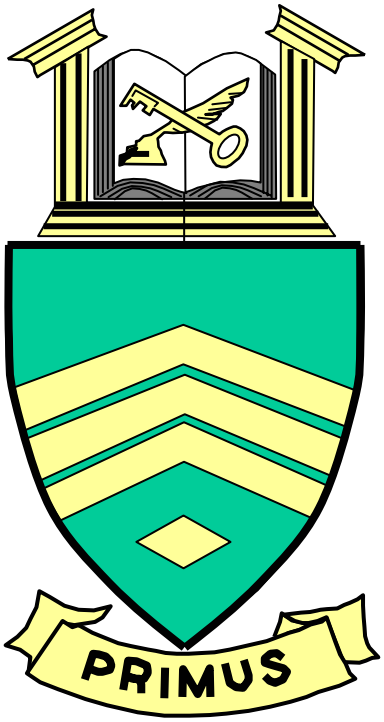
U.S. ARMY SERGEANTS MAJOR ACADEMY (FSC-TATS)

R653 (052002) JUN 01

ENFORCE PERSONNEL SECURITY POLICIES

PRERESIDENT TRAINING SUPPORT PACKAGE



Overview

Personnel security at the unit level can be the first line of defense against security breaches that may effect the national security. During this lesson, you will learn how to enforce personnel security policies within a unit. This lesson includes three Student Handouts, a Lesson Exercise, and a Solution/Discussion for the Lesson Exercise.

Inventory of Lesson Materials

Prior to starting this lesson ensure you received all materials (pages, tapes, disks, etc.) required for this Training Support Package. Go to the "**This [TSP or Appendix] Contains**" section, on page two of the TSP and the first page of each Appendix, and verify you have all the pages. If you are missing any material, contact the First Sergeant Course Class Coordinator at the training institution where you will attend phase II FSC-TATS.

Point of Contact

If you have any questions regarding this lesson, contact the First Sergeant Course Class Coordinator at the training institution where you will attend phase II FSC-TATS.

PRERESIDENT TRAINING SUPPORT PACKAGE

TSP Number /Title	R653 Enforce Personnel Security Policies
Effective date	JUN 01
Supersedes TSPs	R653, Enforce Personnel Security Policies DEC 99
TSP User	This TSP contains a training requirement that you must complete prior to attending phase II, FSC-TATS. It will take you about 1 hour to complete this requirement.
Proponent	The proponent for this document is U.S. Army Sergeants Major Academy. POC: FSC Course Chief, DSN: 978-8329/8848; commercial: (915) 568-8329/8848.
Comments /Recommendations	Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to: ATTN ATSS DCF FSC TATS COMDT USASMA BLDG 11291 BIGGS FLD FT BLISS TX 79918-8002
Foreign Disclosure Restrictions	The lesson developer in coordination with the USASMA foreign disclosure authority has reviewed this lesson. This lesson is releasable to foreign military students from all requesting foreign countries without restrictions.

This TSP Contains

The following table lists the material included in this TSP:

SECTION I ADMINISTRATIVE DATA

Task Trained

This lesson trains the task listed in the following table:

Task number:	301-371-1051
Task title:	Enforce a Personnel Security Program,
Conditions:	as a first sergeant, given AR 380-67,
Standards:	IAW AR AR 380-67.
Task Proponent:	U. S. Army Intelligence Center & Fort Huachuca

Tasks Reinforced

This lesson reinforces the task listed in the following table:

Task number:	704-002-0001
Task title:	Identify leader actions and tools that support the Army Management Control Process,
Conditions:	as a small unit leader or staff officer executing responsibilities in personnel, supply, maintenance, and training functional areas, given AR 11-2,
Standards:	IAW AR 11-2.
Task Proponent:	Army Management Staff College

Prerequisite Lesson

None

Clearance and Access

There is no clearance or access requirement for this lesson.

References

The following table lists reference(s) for this lesson:

Number	Title	Date	Para No.	Additional Information
AR 380-67	Personnel Security Program	9 Sep 88	None	None

Equipment Required

None

Materials Required

None

Safety Requirements

None

Risk Assessment Level

Low

Environmental Considerations

None

Lesson Approval

The following individuals reviewed and approved this lesson for publication and incorporation into the First Sergeant Course--The Army Training System.

Name/Signature	Rank	Title	Date
Kevin L. Graham	MSG	Training Developer	
Chris L. Adams	SGM	Chief Instructor, FSC	
John W. Mayo	SGM	Course Chief, FSC-TATS	

SECTION II INTRODUCTION

Terminal Learning Objective

At the completion of this lesson, you will--

Action:	Identify requirements for enforcement of a unit personnel security program,
Conditions:	as a first sergeant in a classroom environment, given an extract of AR 380-67 (SH-1 & SH-2),
Standard:	Identified requirements for enforcement of a unit personnel security program IAW SH-1 and SH-2.

Evaluation

Before entering phase II FSC-TATS, you will receive the end of Phase I Performance Examination that will include questions based on material in this lesson. On that examination, you must answer at least 70 percent of the questions correctly to achieve a GO.

Instructional Lead-in

Ensuring personnel in your unit are properly cleared for access, to the level needed to accomplish their mission, is a shared responsibility for the first sergeant. It is also a shared task of the first sergeant to ensure that personnel who violate the spirit and intent of the personnel security program have their access to classified information revoked or suspended, in a timely manner.

SECTION III PRESENTATION

ELO 1

Action:	Identify the criteria for access to security information and granting of a security clearance,
Conditions:	as a first sergeant in a classroom environment, given SH-1 and SH-2,
Standard:	Identified the criteria for access to security information and granting of a security clearance IAW SH-1 and SH-2.

Learning Step/Activity (LS/A) 1, ELO 1

To complete this learning step/activity, you are to—

- Read the above ELO.
- Study Student Handouts 1 and 2 (Appendix C).
- Complete Item 1 of the Lesson Exercise (Appendix B).

ELO 2

Action:	Identify the criteria for suspending/revoking access,
Conditions:	as a first sergeant in a classroom environment, given SH-1 and SH-2,
Standard:	Identified the criteria for suspending/revoking access IAW SH-1 and SH-2.

LS/A 1, ELO 2

To complete this learning step/activity, you are to—

- Read the above ELO.
- Review Student Handouts 1 and 2. (Appendix C).
- Complete Items 2, 3, and 4 of the Lesson Exercise (Appendix B).

SECTION IV SUMMARY

Review/ Summarize Lesson	To assist the commander you need to continue to review the procedures and processes in administering to the personnel security program within your unit. Ensuring a viable program will require your direct supervision.
Check on Learning	The Lesson Exercise in Appendix B serves as the Check on Learning.
Transition to Next Lesson	None

SECTION V STUDENT EVALUATION

Testing Requirements	Before entering phase II FSC-TATS, you will receive the end of Phase I Performance Examination that will include questions based on material in this lesson. On that examination, you must answer at least 70 percent of the questions correctly to achieve a GO.

SECTION VI STUDENT QUESTIONNAIRE

Directions Complete the following blocks:

- Enter your name, your rank, and the date you complete this questionnaire.

Name:	Rank:	Date:

- Answer items 1 through 6 below in the space provided.
- Fold the questionnaire so the address for USASMA is visible.
- Print your return address, add postage, and mail.

Note: Your response to this questionnaire will assist the Academy in refining and improving the course. When completing the questionnaire, answer each question frankly. Your assistance helps build and maintain the best Academy curriculum possible.

Item 1	Do you feel you have met the learning objectives of this lesson?
Item 2	Was the material covered in this lesson new to you?
Item 3	Which parts of this lesson were most helpful to you in the learning objectives?
Item 4	How could we improve the format of this lesson?
Item 5	How could we improve the content of this lesson?
Item 6	Do you have additional questions or comments? If you do, please list them here. You may add additional pages if necessary

ATTN ATSS DCF FSC TATS
COMDT USASMA
BLDG 11291 BIGGS FLD
FT BLISS TX 79918-8002

Appendix B

Index of Lesson Exercises and Solutions

This Appendix Contains

This Appendix contains the items listed in this table--

LESSON EXERCISE 1
(Self-Graded)

ENFORCE PERSONNEL SECURITY POLICIES

Reference Materials/ Solutions

- Do not use any reference material or refer to the solution when you complete the items in this lesson exercise. Circle the correct response.

Item 1. What is the exact criteria for entitlement to knowledge of, possession of, or access to classified defense information?

a. Solely by virtue of office, position, grade, rank, and the need to know.

b. Position, grade, and compelling national security reasons.

c. Official military duties require such access and the appropriate security clearance has been granted.

d. Proper degree of security clearance and meet the access parameters within the organization.

Item 2. Commanders must report credible derogatory information to the Commander, Central Clearance Facility on what category of personnel?

a. For all personnel who hold Top Secret clearances.

b. Only if the commander believes the information received is serious.

c. For all personnel regardless of the type/level of clearance held.

d. For all personnel regardless of whether or not they hold any type of clearance.

Item 3. Upon receipt of a Letter of Intent (LOI) from CCF to deny or revoke access, individuals can do which of the following?

a. Respond with an explanation or rebuttal to the LOI.

b. Have the commander decide on action to revoke or suspend access not to exceed 60 days or upon adjudication of the individual's rebuttal, whichever comes first.

c. Voluntarily request suspension of access to classified material until successful resolution of the denial or revocation action.

d. Appeal to their commander to have the derogatory information removed from their Official Personnel Military File (OMPF).

Item 4. With regards to allegations related to disqualification, what type of process would be appropriate on an individual who develops questionable behavior patterns?

a. The unit should initiate a periodic reinvestigation (PR) to ascertain the facts.

b. The unit should request a special investigative inquiry (SII) to resolve issues in doubt.

c. The higher headquarters Security Manager should submit a DD Form 398-2.

d. The unit should request an updated National Agency Check (NAC) and Local Area Check (LAC).

- You may now check your responses to the above items with the Solution/Discussion to Lesson Exercise 1. If your responses do not match the correct responses in the Solution/ Discussion to Lesson Exercise 1, you should study the appropriate references as indicated.

SOLUTION/DISCUSSION FOR LESSON EXERCISE 1
(Self-Graded)

ENFORCE PERSONNEL SECURITY POLICIES

Item 1. What is the exact criteria for entitlement to knowledge, possession of, or access to classified defense information?

c. official military duties require such access, and the appropriate security clearance has been granted.

Ref: SH-2-5 and SH-2-10, AR 380-67, paragraph 2-100b and paragraph 7-102 (ELO 1)

Item 2. Commanders must report credible derogatory information to the Commander, Central Clearance Facility on what category of personnel?

d. For all personnel regardless of whether or not they hold any type of clearance.

Ref: SH-2-11, AR 380-67, paragraph 8-101b(4) (ELO 2)

Item 3. Upon receipt of a Letter of Intent (LOI) from CCF to deny or revoke access, the individual can do which of the following?

a. Respond with an explanation or rebuttal to the LOI.

Ref: SH-2-13 thru SH-2-14, AR 380-67, paragraph 8-201a(2), b, and c (ELO 2)

Item 4. With regards to allegations related to disqualification, what type of process would be appropriate on an individual who develops questionable behavior patterns?

b. The unit should request a special investigative inquiry (SII) to resolve issues in doubt.

Ref: SH-2-7, AR 380-67, paragraph 3-701 (ELO 2)

Appendix C

Index of Student Handouts

This Appendix Contains

This Appendix contains the items listed in this table--

Title/Synopsis	Pages
SH-1, Paraphrased material from AR 380-67	SH-1-1 thru SH-1-6
SH-2, Extract of AR 380-67	SH-2-1 thru SH-2-17
SH-3, Extract of AR 380-5	SH-3-1 thru SH-3-3

Student Handout 1

This Handout

This student handout contains 5 pages (SH-1-2 thru SH-1-6) of paraphrased material to assist you in understanding the elements that a first sergeant should know to assist his or her commander and the unit security manager to perform the important function of the personnel security program. Most of this material comes from AR 380-67. SH-2 is an extract of portions of the AR.

To maintain a viable personnel security program within the unit, the first sergeant should continuously monitor the program to assist the commander and the unit security manager in performing their day-to-day functions. The following represents some of the many topics that may assist you in this endeavor.

■ Do you know what occurs if an individual arrives in your unit without a proper security clearance? You should know the prescribed procedures for obtaining the proper level of clearance. Keep in mind that you will normally do this in conjunction with your unit S1/Personnel Action Center (PAC) and the unit Security Manager.

Security Clearances (para 3-400):

The types (level) and investigative requirements are as follows:

- ***Top Secret*** (para 3-401a)
- ***Secret*** (para 3-401b)
- ***Confidential*** (para 3-401c)

(You should also know that there may be other types of local access requirements to consider, such as NATO, WINTEL, COSMIC, LAA, etc.)

■ Another one of the items you may need to concern yourself with is ensuring personnel in your unit have the correct level of security clearance for their specific duty positions that require access to classified defense information. This could include, as a minimum, checking the Unit Manning Report (UMR), Table of Distribution and Allowances (TDA), Modification Table of Organization and Equipment (MTOE), current unit security clearance roster, or the local personnel security SOP. You may also want to check with the section where the soldier will work, or works, to ensure the requirement for a specific level of access still exists. Again, as stated earlier, you will work with the Security Manager and the S1/PAC to assist the commander in performing this vital function.

Access (para 1-300 & 1-330):

- Defined as the ability and opportunity to obtain knowledge of classified information.
- Mainly as it pertains to having access to classified information in a location where a unit/section stores classified information.
- Only grant personnel security clearances to U.S. citizens (this includes native born, naturalized, derivative birth, and those with a derivative naturalization).

Critical military duties (para 3-703.1):

All military personnel with duties that fall under any of the following criteria:

- Access to Top Secret information.
- Development or approval of plans, policies, or programs that affect the overall operations of the DOD or a Component.
- Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.
- Investigative and certain support duties, adjudication of personnel security clearances or access authorizations, or making personnel security determinations.
- Public contact, or other duties demanding the highest degree of public trust.
- Duties under Special Access programs, excluding controlled nuclear duty positions.
- Category I ADP positions.
- Any other position so designated by the Secretary of the Army (SA) or designee.

■ A part of your function in maintaining a viable personnel security program is to monitor both the initial and periodic personnel security briefings for the unit. You should coordinate with the security manager for scheduling of the appropriate briefings. Integrating them into the short/long range planning calendar will help and could avoid conflicts.

Security Education (para 9-200):

- An integral part of the DOD security program is the indoctrination of individuals on their security responsibilities.
- A unit shall establish and maintain procedures to ensure that personnel receive a periodic briefing on their security responsibilities.
- This remains a requirement for personnel who require access to classified information or who receive an assignment to a position that requires an individual to be trustworthy.

Initial Briefing (para 9-201):

- All persons cleared for access to classified information or assigned to duties requiring trustworthiness will receive an <u>initial</u> security briefing.
- The security office will maintain a record of the briefing.
- As a minimum it should contain the following elements:
  - ♦ Specific security requirements for a soldier's particular job.
  - ♦ Any possible techniques employed by foreign intelligence activities in their attempt to obtain classified information—ensure it includes the soldier's responsibility to report such attempts to the proper authorities (or to the commander) immediately after a suspected contact.

Initial Briefing continued:

♦ The prohibition against disclosing classified information, by any means, to unauthorized persons or discussing or handling classified information in a manner that would make it accessible to unauthorized persons.

♦ Ensure you outline the penalties for security violations. Here are some of the penalties you could include (see SH-3, paragraph 1-21 for this subject):

- warning notice,
- reprimand,
- termination of classification authority,
- suspension without pay,
- forfeiture of pay,
- removal or discharge,
- legal action under the Uniform Code of Military Justice (UCMJ)

Refresher Briefing (para 9-202):

- A unit should have a refresher briefing to provide, at a minimum, annual security training for personnel who have continued access to classified information.

■ Ensure your unit has procedures in place for withdrawal of access should an individual become vulnerable by exploitation to hostile intelligence activities or should he otherwise become untrustworthy. This item is essential to keep a unit from having problems in safeguarding, handling, and maintaining of classified defense information.

Evaluating Security Eligibility (para 9-100):

- AR 380-67 defines this topic as:

"A personnel security determination is an effort to assess the future trustworthiness of an individual in terms of the likelihood of an individual preserving the national security."

- It further states that "there is a need to ensure that, after the personnel security determination is reached, the individual's trustworthiness is a matter of continuing assessment."
- There are many persons involved in the process of assessing the individual:
  - ♦ the organizational commander or manager,
  - ♦ the individual's supervisor,
  - ♦ the individual himself/herself,
  - ♦ and just as important, the first sergeant.

Evaluating Security Eligibility continued:

- The evaluation process also includes close coordination with the following:
  - ♦ security authorities,
  - ♦ personnel (S1/PAC),
  - ♦ medical,
  - ♦ legal,
  - ♦ supervisors.
- An individual's responsibility entails reporting **(para 9-103):**
  - ♦ any contact, intentional or otherwise, (outside official duties) with citizens from certain foreign countries (appendix H contains a complete listing),
  - ♦ attempts by representatives or citizens of the countries listed in appendix H to cultivate friendships or place the individual under obligations,
  - ♦ the offering of any money payments or bribery to obtain information of actual or potential intelligence value,
  - ♦ attempts to coerce by blackmail or by threats,
  - ♦ all foreign travel, in advance,
  - ♦ any information considered derogatory in nature (see para 2-200 for specific areas in this category).
- There is also a coworkers responsibility **(para 9-104):**
  - ♦ to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified defense information, or employed in a sensitive position.

■ When you receive credible derogatory information on an individual in your unit, you should assist the commander to monitor the process for suspension or revocation of access. You should know the specific reasons why the commander must submit DA Form 5248-R (Report of unfavorable information for security determination) to the CCF. Conduct a systematic/periodic check of each possible source for credible derogatory information for members of your unit (i.e., MP/CID reports, blotter entries; courts martial/article 15s; medical reports/psychiatric exams; letters of indebtedness/reprimand; absence without leave (AWOL) and drug/alcohol incidents).

Unfavorable Administrative Actions (para 8-100):

- For the purposes of AR 380-67, an unfavorable administrative action includes:
  - ♦ any adverse action taken as a result of a personnel security determination,
  - ♦ any unfavorable personnel security determination,
- Whenever credible derogatory information becomes available to the first sergeant, he should expeditiously refer it to the commander or security officer of the organization.

Unfavorable Administrative Actions continued:

- The commander will forward a DA Form 5248-R (Report of Unfavorable Information for Security Determination) to the Commander, CCF (PCCF-M) stating the circumstances.
- As a minimum the initial report will indicate the details of the credible derogatory information and actions taken to resolve the issue (for example, conducting an inquiry or investigation).
- The commander must submit follow-up reports at 90-day intervals if no final action or action remains pending by civil court.

■ You know the rights and responsibilities of individuals pending suspension/revocation and how they may respond to any allegations. You should also check to ensure the individual no longer holds a duty position which requires handling/observing classified defense information, until the final determination arrives from the Commander, CCF. If necessary, monitor the suspense dates for submission of all associated paperwork.

Unfavorable Administrative Action Procedures (para 8-201):

- The Commander, CCF will forward a letter of intent (LOI) through the command security manager to the individual.
- The LOI will outline the derogatory information and explain the proposed action.
- The LOI will also offer the individual the chance to reply in writing, with an explanation, rebuttal, or mitigation for the incident(s).
- The LOI will direct suspension of access to classified defense information.
- The commander will ensure the individual receives counseling as to the seriousness of any contemplated action by CCF.
- The person may seek advice from SJA (or other lawyer at own expense).
- The person's response must address each issue raised in the LOI from CCF.
- If the person requires an extension of the 60-day suspension, the command security manger should forward a request, citing the justification, to the CCF. The request should also include an expected completion date.
- The decision from CCF, forwarded through the command security office to the individual, will be final.

■ For a more comprehensive explanation of the personnel security program, you should obtain AR 380-67, and keep it together with your unit personnel security Standing Operating Procedure (SOP) for reference whenever the need arises.

Student Handout 2

Extract This student handout contains 16 pages (SH-2-2 thru SH-2-17) of material extracted from AR 380-67, Personnel Security Program, downloaded from the United States Army Publishing Agency (USAPA).

TABLE OF CONTENTS

[SHOWS ONLY THOSE PARAGRAPH NUMBERS AND TITLES EXTRACTED FOR THIS STUDENT HANDOUT]

Chapter 1.0 General Provisions

Section III Definitions

1.300 Access

The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures that are in force do not prevent him from gaining know-ledge of such information.

1.301 Adverse action

A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction in pay, or furlough of 30 days or less.

1.302 Background Investigation (BI)

A personnel security investigation consisting of both record reviews and interviews with sources of information as prescribed in paragraph B-3, appendix B, this regulation, covering the most recent 5 years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least the last 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

1.303 Classified information

Official information or material that requires protection in the interests of national security and that is classified for such purpose by appropriate classifying authority in accordance with the provisions of Executive Order 12356 (reference (j)).

1.306 Entrance National Agency Check (ENTNAC)

A personnel security investigation scoped and conducted in the same manner as a National Agency Check except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

1.310.1 Local records check (LRC)

A review of local personnel, post military police, medical records, and other security records as appropriate.

1.312 National Agency Check (NAC)

A personnel security investigation consisting of a records review of certain national agencies as prescribed in paragraph 1, appendix B, this regulation, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

1.312 National Agency Check (NAC)

A personnel security investigation consisting of a records review of certain national agencies as prescribed in paragraph 1, appendix B, this regulation, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

1.314 DOD National Agency Check and written inquiries (DNACI)

A personnel security investigation conducted by the Defense Investigative Service (DIS) for access to SECRET information consisting of a NAC, a credit bureau check, and written inquiries to current and former employers (see para **B-**2, app B), covering a 5-year scope.

1.317 Periodic reinvestigation (PR)

An investigation conducted every 5 years for the purpose of updating a previously completed background or special background investigation on persons occupying positions referred to in paragraphs 3-700 through 3-711. The scope will consist of a personal interview, NAC, LACs, credit bureau checks, employment records, employment references and developed character references and will normally not exceed the most recent 5-year period.

1.320 Security clearance

A determination that a person is eligible under the standards of this regulation for access to classified information.

1.325 Special background investigation (SBI)

A personnel security investigation consisting of all of the components of a BI plus certain additional investigative requirements as prescribed in paragraph B- 4, appendix B, this regulation. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

1.328 Unfavorable administrative action

Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations as defined in this regulation.

1.329 Unfavorable personnel security determination

A denial or revocation of clearance for access to classified information; denial or revocation of access to classified information; denial or revocation of a Special Access authorization (including access to SCI); retention, nonappointment to or nonselection for appointment to a

sensitive position; retention, non-appointment to or nonselection for any other position requiring a trustworthiness determination under this regulation; reassignment to a position of lesser sensitivity or to a non-sensitive position; and nonacceptance for or discharge from the Armed Forces when any of the foregoing actions are based on derogatory information of personnel security significance.

1.330 United States citizen

a. Native born. A person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Marina Islands; U.S. Virgin Islands; or Panama Canal Zone (if the father or mother (or both) was or is a citizen of the United States).

b. Naturalized. **A person born outside of the United States who has completed naturalization procedures and has been given U.S. citizenship by duly constituted authority.**

***c. Derivative birth*.** **A person born outside the United States who acquires U.S. citizenship at birth because one or both of his or her parents are U.S. citizens at the time of the person's birth.**

d. Derivative naturalization. **A person who acquires U.S. citizenship after birth through naturalization of one or both parents.**

Chapter 2.0 Policies

2.100 General

a. Only U.S. citizens shall be granted a personnel security clearance, assigned to sensitive duties, or granted access to classified information unless an authority designated in appendix F has determined that, based on all available information, there are compelling reasons in furtherance of the Department of Defense mission, including, special expertise, to assign an individual who is not a citizen to sensitive duties or grant a limited access authorization to classified information. Non-U.S. citizens may be employed in the competitive service in sensitive civilian positions only when specifically approved by the Office of Personnel Management, pursuant to Executive Order 11935 (reference (k)). Exceptions to these requirements shall be permitted only for compelling national security reasons.

b. **No person is entitled to knowledge of, possession of, or access to classified defense information solely by virtue of office, position, grade, rank, or security clearance. Such information will be entrusted only to persons whose official military or other governmental duties require it and who have been investigated and cleared for access under the standards prescribed by this regulation. Security clearances indicate that the persons concerned are eligible for access to classified information should their official duties require it.**

2.101 Clearance and sensitive position standard

The personnel security standard that must be applied to determine whet-her a person is eligible for access to classified information or assignment to sensitive duties is whether, based on all available information, the person's loyalty, reliability, and trustworthiness are such that en-trusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

2.102 Military service standard

The personnel security standard that must be applied in determining whether a person is suitable under national security criteria for appointment, enlistment, induction, or retention in the Armed Forces is that, based on all available information, there is no reasonable basis for doubting the person's loyalty to the Government of the United States.

2.200 Criteria for application of security standards

The ultimate decision in applying either of the security standards set forth in paragraphs 2-101 & 2-102, above, must be an overall common sense determination based upon all available facts. The criteria for determining eligibility for a clearance or assignment to a sensitive position under the security standard shall include, but not be limited to the following:

a. Commission of any act of sabotage, espionage, treason, terrorism, anarchy, sedition, or attempts there-at or preparation therefor, or conspiring with or aiding or abetting another to commit or attempt to commit any such act.

b. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist, or with an espionage or other secret agent or similar representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

c. Advocacy or use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

d. Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in any foreign or domestic organization, association, movement, group or combination of persons (hereafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent

others from exercising their rights under the Constitution or laws of the United States or of any State or which seeks to overthrow the Government of the United States, or any State or subdivision thereof by unlawful means.
e. Unauthorized disclosure to any person of classified information, or of other information, disclosure of which is prohibited by statute, Executive order, or regulation.
f. Performing or attempting to per-form one's duties, acceptance and active maintenance of dual citizen-ship, or other acts conducted in a manner which serves or which could be expected to serve the interests of another government in preference to the interests of the United States.
g. Disregard of public law, statutes, Executive orders, or regulations, including violation of security regula-tions or practices.
h. Criminal or dishonest conduct.
i. Acts of omission or commission that indicate poor judgment, unreliability or untrustworthiness.
j. Any behavior or illness, in-cluding any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such case.
k. Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be (1) the presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation (or areas under its domination) whose interests may be inimical to those of the United States, or (2) any other circumstances that could cause the applicant to be vulnerable.
l. Excessive indebtedness, recurring financial difficulties, or unexplained affluence.
m. Habitual or episodic use of in-toxicants to excess.
n. Illegal or improper use, possession, transfer, or sale of or ad-diction to any controlled or psychoactive substance, narcotic, cannabis, or other dangerous drug.
o. Any knowing and willful falsification, cover-up, concealment, mis-representation, or omission of a material fact from any written or oral statement, document, form or other representation or device used by the Department of Defense or any other Federal agency.
p. Failing or refusing to answer or to authorize others to answer questions or provide information required by a congressional committee, court, or agency in the course of an official inquiry whenever such answers or information concern relevant and material matters pertinent to an evaluation of the individual's trustworthiness, reliability, and judgment. Refusing or intentionally failing to provide a current personal security question-naire (PSQ) or omitting material facts in a PSQ or other security form. Refusing to submit to a medical or psychological evaluation when information indicates the individual may have a mental or nervous disorder or be addicted to alcohol or any controlled substance.
q. Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment, or lack of regard for the laws of society.

Chapter 3.0 Personnel Security Investigative Requirements
Section-IV - Security Clearance
3.400 General
a. The authorities designated in paragraph F-1, appendix F, are the only authorities authorized to grant, deny or revoke DOD personnel security clearances. The granting of such clearances shall be limited to only those persons who require access to classified information for mission accomplishment.
b. Military, DOD civilian, and con-tractor personnel who are employed by or serving in a consultant capacity to the DOD, may be considered for access to classified information only when such access is required in connection with official duties. Such individuals may be granted either a final or interim personnel security clearance provided the investigative requirements set forth below are complied with, and provided further that all available information has been adjudicated and a finding made that such clearance would be clearly consistent with the interests of national security.
c. Before issuing any security clearance, final or interim, the commander must verify the following:
(1) That the person has had no break in Federal service exceeding 12 months since the completion of the investigation.
(2) That the person can prove U.S. citizenship by presenting one of the documents listed in para-graph B-4d, appendix B (see paragraph 3-402).

3.401 Investigative requirements for clearance

a. TOP SECRET.
(1) Final clearance:
(a) BI/SBI.
(b) Established billet per paragraph 3-104 (except contractors).
(c) Favorable review of local personnel, post military police, medical records, and other security records as appropriate.
(2) Interim clearance:
(a) Favorable NAC, ENTNAC, DNACI, or NACI completed within past 5 years.
(b) Favorable review of DD Form 398/SF-86/SF-171/DD Form 49.
(c) BI or SBI has been initiated.
(d) Favorable review of local personnel, post or base military police,

medical, and other security records as appropriate.
(e) Established billet per paragraph 3-104 (except contractors).
(f) Provisions of paragraph 3-204 have been met regarding civilian personnel.
(g) If evidence exists of a BI, SBI, full field investigation, CID character investigation, or comparable investigation not over 4½ years old, provisions of subparagraphs (b) and (c) above are waived and a DA Form 5247-R (Request for Security Determination) requesting a final TOP SECRET clearance will be submitted to CCF noting that an interim clearance was granted. Such evidence will be attached to the DA Form 5247-R. CCF will check the DCII to find whether or not a later investigation exists that would require withdrawal of a security clearance.
(h) Commanders may grant an interim TOP SECRET clearance for 180 days in the name of the Commander, CCF.
b. SECRET.
(1) Final clearance:
(a) DNACI: Military (except first-term enlistees) and contractor employees.
(b) NACI: Civilian employees.
1. NACI is required even though the individual held a valid security clearance based on a NAC, ENTNAC, or DNACI while a member of the Armed Forces.
2. Exception: Summer hires, members of cooperative education programs, employees of non-appropriated fund instrumentalities, Army and Air Force Exchange Service employees, Red Cross members, USO employees, and non-Federal employees of the Army National Guard may be granted a final clearance on the basis of a favorable completed NAC/ENTNAC conducted by the DIS. No interim clearance is authorized for these employees.
(c)Entrance: First-term enlistees.
(d) Favorable review of local personnel, post military police, medical, and other security records as appropriate.
(2) Interim clearance:
(a) When a valid need to access SECRET information is established, an interim SECRET clearance may be issued for 180 days in the name of the Commander, CCF, in every case, provided that a DA Form 5247-R has been submitted to CCF, and the steps outlined in subparagraphs (b) thru (e) below, have been complied with.
(b) Favorable review of DD Form3 98-2/SF 85/SF 171/DD Form 48.
(c) NACI, DNACI, or ENTNAC initiated.
(d) Favorable review of local personnel, post or base military police, medical, and other security records as appropriate.
(e) NAC or ENTNAC completed or, in an emergency, provisions of paragraph 3-204 have been com-plied with regarding civilian personnel.
c. CONFIDENTIAL.
(1) Final clearance:
(a) NAC or ENTNAC: Military and contractor employees (except for Philippine national members of the United States Navy on whom a BI shall be favorably completed).
(b) NACI; Civilian employees (except for summer hires and others listed in para 3-401b(l)(b)(l) 2 who may be granted a final clearance on the basis of a NAC).
(c) Favorable review of local personnel, post military police, medical, and other security records as appropriate.
(2) Interim clearance:
(a) Favorable review of DD Form 398-2/SF 86/SF 171/DD Form 48.
(b) NAC, ENTNAC, or NACI initiated.
(c) Favorable review of local personnel, post or base military police, medical, and other security records as appropriate.
(d) Provisions of paragraph 3-204 have been complied with regarding civilian personnel.
d. Validity of, previously granted clearances.
Clearances granted under less stringent investigative requirements retain their validity; however, if a higher degree of clearance is required, investigative requirements of this regulation will be followed.

Section VII Reinvestigation
3.701 Allegations related to disqualification

Whenever questionable behavior patterns develop, derogatory information is discovered, or inconsistencies arise related to the disqualification criteria outlined in paragraph 2-200 that could have an adverse impact on an individual's security status, a special investigative inquiry (SII), psychiatric, drug, or alcohol evaluation, as appropriate, may be requested to resolve all relevant issues in doubt. If it is essential that additional relevant personal data is required from the investigative subject and the subject fails to furnish the required data, the subject's existing security clearance or assignment to sensitive duties shall be terminated in accordance with paragraph 8-201 of this regulation.

3.703.1 Critical military duties

All military personnel with a military occupational speciality (MOS) or specialty classification under AR 611-101 (reference (zz)), AR 611-112 (reference (aaa)), or AR 611-201 (reference (bbb)) that requires eligibility for SCI, regardless of access level, shall be the subject of a PR on a 5-year recurring basis as set forth in paragraph B-5, appendix B. So will military personnel with duties that fall under any of the following criteria:
a. Access to TOP SECRET information.

b. Development or approval of plans, policies, or programs that affect the overall operations of the DOD or a Component.
c. Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.
d. Investigative and certain sup-port duties, adjudication of personnel security clearances or access authorizations, or making personnel security determinations.
e. Fiduciary, public contact, or other duties demanding the highest degree of public trust.
f. Duties falling under Special Access programs (excluding controlled nuclear duty positions).
g. Category I ADP positions.
h. Any other position so designated by the Secretary of the Army (SA) or designee.

Chapter 5.0 Requesting Personnel Security Investigations

5.106 Requests for additional information or clarification

When questionable behavior, inconsistencies, or other derogatory information related to the criteria in paragraph 2-200 arise, CCF may request more information or clarification directly from the field commander or the subject (see para 3-701). Such re-quests include, but are not limited to the following:
a. Results of command inquiries and investigations; copies of courts- martial proceedings; copies of administrative or disciplinary actions, written reprimands, Articles 15; results of local records file checks or of previous psychiatric or drug and alcohol evaluations; or letters of indebtedness received by the command.
b. DD Forms 398, fingerprint cards, and other forms or release statements required to conduct investigations; verification of citizenship of the subject and/or immediate family. Occasionally, to expedite the decision making process, CCF will ask security managers to obtain specific information from the subject, such as current financial status, proof of payment of delinquent debts, or clarification of information listed on DD Form 398 or similar forms.
c. Progress and final reports from Alcohol and Drug Abuse Prevention and Control Program (ADAPCP) officials on alcohol and drug rehabilitation treatment. Such reports will include history and extent of substance abuse, diagnosis, attitude toward treatment, results of treatment, and immediate and long-term prognosis. CCF will request a current alcohol or drug evaluation when incidents of alcohol or drug abuse are reported and the subject has not been referred for drug and/or alcohol treatment; more than 1 year has passed since treatment occurred, or it occur-red during a previous assignment and results are not available; or there was an indication of sub-stance abuse after completion of treatment. A physician or mental health clinician trained in the alcohol and drug rehabilitation field, who is employed by or under contract to the U.S. military or U.S. Government, will conduct the evaluation. The purpose of the evaluation is to assess the subject's ability to refrain from abuse and to obtain an opinion on the potential impact upon the subject's judgment and reliability in protecting classified information and material.
d. Information from medical records that indicates mental disorder or emotional instability or results of any psychiatric or mental health evaluation or treatment for a mental condition. When any information indicates a history of mental or nervous disorder or re-ported behavior appears to be abnormal, indicating impaired judgment, reliability, or maturity, CCF will request a mental health evaluation to determine whether or not any defect in judgment or reliability or any serious behavior disorder exists. A board-certified or board-eligible psychiatrist or licensed or certified clinical psychologist who is employed by or under contract to the U.S. military or U.S. Government will conduct mental health evaluations for security clearance purposes. The evaluation report should out-line the methods used in the evaluation (for example, psychological testing and clinical inter-views), include a narrative case history, assess the results of any psychological tests, and include a diagnosis under DSM III (see note) or state that no diagnosis exists. The report should include a prognosis and indicate what effect the diagnosed condition has on judgment, reliability, and stability, and describe any characteristics in a normal or stressful situation. If the individual's condition is under control through treatment or medication, the re-port should indicate what could happen if the individual did not comply with treatment and what likelihood exists of failure to comply. If appropriate, the report should indicate an estimated time or condition that could cause a favorable change.
Note. American Psychiatric Association: Diagnostic and Statistical Manual of Mental Disorders, Third Edition, Wash, DC: APA,1980.
e. It is imperative, in the interests of national security, that the commander and the subject of the case respond promptly to CCF's request for information. Failure to respond to requests for information required by CCF for personnel security clearance de-

terminations within the prescribed time shall result in CCF directing suspension of the individual's access to classified information or termination of action to process request for security clearance. Continued failure to respond to CCF's request for information shall result in action to terminate the individual's security clearance utilizing the procedures of para-graph 8-201.

Chapter 6.0 Adjudication

6.101 Central adjudication

a. To ensure uniform application of the requirement of this regulation and to ensure that DOD personnel security determinations are effected consistent with existing statutes and Executive orders, the head of each Military Department and Defense Agency shall establish a single central adjudication facility for his or her Component. The CCF, Fort George G. Meade, MD, has been designated as the single central adjudication facility for the DA. The function of each facility or the CCF shall be limited to evaluating personnel security investigations and making personnel security de-terminations. The Chief of each central adjudication facility or Commander, CCF, shall have the authority to act on behalf of the head of the Component or the SA with respect to personnel security determinations. All information relevant to determining whether a per-son meets the appropriate personnel security standard prescribed by this regulation shall be reviewed and evaluated by personnel security specialists specifically designated by the head of the Component con-cerned, or designee, or by the SA or the DCSINT.

b. In view of the significance each adjudicative decision can have on a person's career and to ensure the maximum degree of fairness and equity in such actions, a minimum level of review shall be required for all clearance/access determinations related to the following categories of investigations:

(1) *BI/SBI/PR/ENAC/SII:*

(a) *Favorable*: Completely favorable investigations shall be re-viewed and approved by an adjudicative official in the civilian grade of GS-7/9 or the military rank of O-3.

(b) *Unfavorable*: Investigations that are not completely favorable shall undergo at least two levels of re-view by adjudicative officials, the second of which must be at the civilian grade of GS-11/12 or the military rank of O-4. When an unfavorable administrative action is contemplated under paragraph 8-201, the letter of intent (LOI) to deny or revoke must be approved and signed by an adjudicative official at the civilian grade of GS-13/14 or the military rank of O-5. A final notification of unfavorable administrative action, subsequent to the issuance of the LOI, must be approved and signed at the civilian grade of GS-14/15 or the military rank of O-6.

(2) *NACI/DNACI/NAC/ENTNAC*:

(a) *Favorable*: A completely favorable investigation may be finally adjudicated after one level of re-view provided that the decision making authority is at the civilian grade of GS-5/7 or the military rank of O-2.

(b) *Unfavorable*: Investigations that are not completely favorable must be reviewed by an adjudicative official in the civilian grade of GS-7/9 or the military rank of O-3. When an unfavorable administrative action is contemplated under para-graph 8-201, the letter of intent to deny / revoke must be signed by an adjudicative official at the civilian grade of GS-11/12 or the military rank of O-4. A final notification of unfavorable administrative action subsequent to the issuance of the LOI must be signed by an adjudicative official at the civilian grade of GS-13 or the military rank of O-5 or above.

c. Exceptions to the above policy may only be granted by the Deputy Under Secretary of Defense for Policy.

6.102 Evaluation of personnel security information

a. The criteria and adjudicative policy to be used in applying the principles at paragraph 6-100, above, are set forth in paragraph 2-200 and appendix I of this regu-lation. The ultimate consideration in making a favorable personnel security determination is whether such determination is clearly con-sistent with the interests of national security and shall be an overall common sense evaluation based on all available information. Such a determination shall include consideration of the following factors:

(1) The nature and seriousness of the conduct;

(2) The circumstances surrounding the conduct;

(3) The frequency and recency of the conduct;

(4) The age of the individual;

(5) The voluntariness of participation; and

(6) The absence or presence of rehabilitation.

b. Detailed adjudication policy guidance to assist adjudicators in determining whether a person is eligible for access to classified information or assignment to sensitive duties is contained in appendix I. Adjudication policy for access to SCI is contained in DCID1/14.

Chapter 7.0 Issuing Clearance and Granting Access

7.100 General

a. The issuance of a personnel security clearance (as well as the function of determining that an individual is eligible for access to Special Access program information, or is suitable for assignment to sensitive duties or such other duties that require a trustworthiness determination) is a function distinct from that involving the granting of access to classified information. Clearance determinations are made on the

merits of the individual case with respect to the subject's suitability for security clearance. Access determinations are made solely on the basis of the individual's need for access to classified information in order to perform official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for cause without applying the provisions of paragraph 8-201.

b. Only the authorities designated in paragraph F-1, appendix F, are authorized to grant, deny or revoke personnel security clearances or Special Access authorizations (other than SCI). Any commander or head of an organization, to include CCF, may suspend access for cause when there exists information raising a serious question as to the individual's ability or intent to protect classified information, provided that the procedures set forth in para-graph 8-102 of this regulation are complied with.

c. All commanders and heads of DOD organizations have the responsibility for determining those position functions in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of this regulation.

7.102 Granting access

a. Access to classified information shall be granted to persons whose official duties require such access, and who have the appropriate personnel security clearance. CCF normally grants the highest level of clearance authorized by the personnel security investigation on record. Access determinations (other than for Special Access pro-grams) are not an adjudicative function relating to an individual's suitability for such access. Rather they are decisions made by the commander that access is officially required.

b. In the absence of derogatory information on the individual concerned, DOD commanders and organizational managers shall accept a personnel security clearance determination, issued by any DOD authority authorized by this regulation to issue personnel security clearances, as the basis for granting access, when access is required, without requesting additional investigation or investigative files. For Army-affiliated personnel, this determination is documented by a DA Form 873 in the personnel file. A DA Form 873, as well as clearance certificates issued by other DOD Components, will be honored provided—

(1) There has been no break in Federal service exceeding 12 months since the investigation date; and

(2) A check of local records discloses no unfavorable information.

c. The access level of cleared individuals will also be entered into the DCSI by the Commander, CCF, along with clearance eligibility status, as systems are developed and adopted which make such actions feasible.

d. Once the Commander, CCF, has granted a person's security clearance, special access for NATO, SIOP-ESI, or other pro-grams will be granted by the commander responsible for their control under appropriate regulations. The Commander, CCF, will make all eligibility determinations for SCI access.

e. DA Form 5247-R, with a copy of the clearance documentation, will be forwarded to CDR, CCF (PCCF-M), when accepting an Army clearance granted prior to CCF's assumption of clearance authority or by another DOD Component or Federal agency. In these cases, access to classified information need not be delayed pending receipt of a DA Form 873. Access may be granted and continued provided local file checks are favorable. Forwarding is not necessary if DA Form 873 is annotated, "Project Top Feed Completed."

Chapter 8.0 Unfavorable Administrative Actions

Section-I Requirements
8.100 General

For purposes of this regulation, an unfavorable administrative action includes any adverse action which is taken as a result of a personnel security determination, as defined at paragraph 1-301, and any unfavorable personnel security determination, as defined at paragraph 1-329. This chapter is intended only to provide guidance for the internal operation of the Department of Defense and is not intended to, does not, and may not be relied upon, to create or enlarge the jurisdiction or review authority of any court or administrative tribunal, including the Merit Systems Protection Board.

8.101 Referral for action

a. Whenever derogatory information relating to the criteria and policy set forth in paragraph 2-200 and appendix I of this regulation is developed or otherwise becomes available to any DOD element, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty. The commander or security officer of the organization to which the subject of the information is assigned shall review the information in terms of its security significance and completeness. If further information is needed to confirm or disprove the allegations, additional investigation

should be requested. The commander of the duty organization shall ensure that the parent Component of the individual concerned is informed promptly concerning (1) the derogatory information developed and (2) any actions taken or anticipated with respect thereto by forwarding DA Form 5248-R (Report of Unfavorable Information for Security Determination) to the Commander, CCF (PCCF-M). However, referral of derogatory information to the commander or security officer shall in no way affect or limit the responsibility of the central adjudication facility to continue to process the individual for denial or revocation of clearance or access to classified information, in accordance with paragraph 8-201, below, if such action is warranted and supportable by the criteria and policy contained in paragraph 2-200 and appendix I. No unfavorable administrative action as defined in paragraphs 1-328 and 1-329 may be taken by the organization to which the individual is assigned for duty without affording the person the full range of protections contained in paragraph 8-201, below, or, in the case of SCI, Annex B, DCID 1/14 (reference (l)).

b. The Director, DIS, shall establish appropriate alternative means whereby information with potentially serious security significance can be reported other than through DOD command or industrial organization channels. Such access shall include utilization of the DOD Inspector General "hotline" to receive such reports for appropriate follow-up by DIS. DOD Components and industry will assist DIS in publicizing the availability of appropriate reporting channels. Additionally, DOD Components will augment the system when and where necessary. Heads of DOD Components will be notified immediately to take action if appropriate.

(1) When the commander learns of credible derogatory information on a member of his or her command that falls within the scope of paragraph 2-200, the commander will immediately for-ward DA Form 5248-R to the Commander, CCF.

(2) DA Form 5248-R will be submitted in a timely manner. At a minimum, initial reports will indicate the details of the credible derogatory information and actions being taken by the commander or appropriate authorities (for example, conducting an inquiry or investigation) to resolve the incident. Follow-up reports will be submitted at 90-day intervals if the commander has not taken final action or, for ex-ample, the subject is still pending action by civil court. At the conclusion of the command action, a final report will be forwarded to CCF indicating the action taken by the commander. The final report must contain results of any local inquiry, investigation, or board action and recommendation of the command concerning restoration or revocation of the person's security clearance, if appropriate.

(3) Commanders will not delay any contemplated personnel action while awaiting final action by CCF. The personnel action should proceed, with CCF being informed of the final action by submission of DA Form 5248-R through established channels.

(4) If the personnel file does not indicate the existence of a security clearance, commanders must still report information that falls within the scope of paragraph 2-200, since the person might later require a clearance. Only a final report is required on personnel who do not have a security clearance.

(5) SSOs are charged with protecting SCI. If an SSO learns of any derogatory information falling within the scope of paragraph 2-200 concerning any person under the SSO's security cognizance, the SSO will immediately inform the commander. The failure of a commander to forward a DA Form 5248-R to CCF, when derogatory information has been developed on SCI indoctrinated individuals, should be brought to the attention of the individual's security manager and the Senior Intelligence Officer (SIO).

8.102 Suspension

The commander or head of the organization shall determine whether, on the basis of all the facts available upon receipt of the initial derogatory information, it is in the interests of national security to continue subject's security status unchanged or to take interim action to suspend subject's access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), if information exists which raises serious questions as to the individual's ability or intent to protect classified information, until a final determination is made by the appropriate authority designated in appendix F. Every effort shall be made to resolve a suspension action as expeditiously as possible.

a. When a commander learns of significant derogatory information falling within the scope of paragraph 2-200, in addition to the reporting requirements of 8-101a, above, the commander must decide whether or not to suspend the individual's access to classified information. The commander may wish to suspend access on an "informal" basis while gathering information to determine whether or not formal suspension is warranted. After gathering the required data, the commander may

decide to restore access. If the commander does not suspend access, CCF will review all available information and, if warranted, advise the commander to suspend access.

b. If the commander decides on formal suspension of access, DA Form 873 will be removed from individual's personnel file and attached to DA Form 5248-R reporting the suspension to CCF. Once this is done, the commander may not restore access until a final favorable determination by the Commander, CCF, unless ALL the following criteria are met. These following procedures apply to both collateral and SCI access:

(1) If the commander determines that the person has been cleared of all charges and that the alleged offense or disqualifying information has been disproved or found groundless, and the commander is completely convinced that no element of risk remains, the commander may restore interim access in the name of the Commander, CCF. The commander will notify CCF of this action. Access will not normally be restored in cases where factors such as dismissal of charges, acquittal because of legal technicalities, plea bargaining, or absence of a speedy trial are involved. These factors cannot be construed as a clearing of all charges.

(2) When the commander is considering suspending or has suspended a person's access be-cause of a suspected or actual psychological problem, the commander may elect to retain the person in status or reinstate access if the following conditions are met:

(a) A current medical evaluation indicates the condition was a one-time occurrence.

(b) The condition has no lasting effects that would affect the person's judgment.

(c) There is no requirement for further medical consultation relating to the condition.

(d) The examining physician recommends the person be returned to full duty status.

(e) The person exhibits no unacceptable behavior after the favorable medical evaluation.

(f) The commander firmly believes the person does not pose a risk to the security of classified information.

(3) If the commander has any doubts concerning the person's current acceptability for access, even though the above provisions have been met, the case will be referred to CCF. Only the Commander, CCF, may reinstate access in cases where the person attempted suicide.

c. The commander will ensure that the SSO is expeditiously notified of any information within the scope of paragraph 2-200 if the person is indoctrinated for SCI. This notification is especially critical if the commander suspends access.

d. A commander who suspends access to classified information will ensure that the suspension is documented in the Field Deter-mined Personnel Security Status data field of the Standard Installation/Division Personnel System personnel file.

8.103 Final unfavorable administrative actions

The authority to make personnel security determinations that will result in an unfavorable administrative action is limited to those authorities designated in appendix F, except that the authority to terminate the employment of a civilian employee of a Military Department or Defense Agency is vested solely in the head of the DOD Component concerned and in such other statutory official as may be designated. Action to terminate civilian employees of the Office of the Secretary of Defense and DOD Components, on the basis of criteria listed in paragraphs 2-200, a through f, shall be coordinated with the Deputy Under Secretary of Defense for Policy prior to final action by the head of the DOD Component. DOD civilian employees or members of the Armed Forces shall not be removed from employment or separated from the Service under provisions of this regulation if removal or separation can be effected under OPM regulations or administrative (non-security) regulations of the Military Departments. However, actions contemplated in this regard shall in no way affect or limit the responsibility of the central adjudication facility to continue to process the individual for denial or revocation of a security clearance, or access to classified information on or assignment to a sensitive position if war-ranted and supportable by the criteria and standards contained in this regulation

Section II Procedures
8.200 General

No final personnel security determination shall be made on a member of the Armed Forces, an employee of the Department of Defense, a consultant to the Department of Defense, or any other person affiliated with the Department of Defense without granting the individual concerned the procedural benefits set forth in 8-201 below, when such determination results in an unfavorable administrative action (see para 8-100). As an exception, Red Cross/United Service Organizations employees shall be afforded the procedures prescribed by DOD Directive 5210.25 (AR 380-49) (reference (w)).

8.201 Unfavorable administrative action procedures

Except as provided for below, no unfavorable administrative action shall be taken under the authority of this regulation unless the person concerned has been given:

a. A written statement of the reasons why the unfavorable administrative action is being taken. The statement shall be as comprehensive and detailed as the protection of sources afforded confidentiality under the provisions of the Privacy Act of 1974 (5 U.S.C.552a) (reference (m)) and national security permit. Prior to issuing a statement of reasons to a civilian employee for suspension or removal action, the issuing authority must comply with the provisions of Federal Personnel Manual, chapter 732, subchapter 1, paragraph 1-6b (reference (cc)). The signature authority must be as provided for in paragraph 6-101b(1)(b) and 6-101b (2)(b).

(1) The Commander, CCF, is the DA authority for denial and/or revocation of security clearances and/or SCI access eligibility. The Commander, CCF, may delegate this authority to those individuals outlined in paragraph 6-101b.

(2) When CCF receives credible derogatory information and denial or revocation of a security clearance and/or SCI access eligibility is considered appropriate, CCF will forward a letter of intent through the command security manager to the individual. This LOI will outline the derogatory information and explain the proposed action. It will offer the person a chance to reply in writing with an explanation, rebuttal, or mitigation for the incidents.

(3) The LOI will direct suspension of access to classified information. If the LOI addresses SCI access only, access to collateral information may continue.

(4) If the person needs access to classified information in order to prepare a response to the LOI, CCF may authorize limited access for that specific purpose.

(5) When a commander receives an LOI concerning a person who is no longer assigned to the command, one of the following actions will be taken:

(a) If the person is transferred, endorse the LOI to the gaining command and forward an information copy of the endorsement to CCF (PCCF-M).

(b) If the person has been released from active duty and has a Re-serve obligation, forward the LOI to the U.S. Army Reserve Personnel Center, ATTN: DARP-SPI, St. Louis, MO 63132-5200. Forward an information copy of the endorsement to CCF (PCCF-M).

(c) If the person has been discharged from military service with no Reserve obligation, endorse the LOI to CCF (PCCF-M), attaching a copy of the discharge orders.

(6) The Commander, CCF, may waive the due process requirements of this chapter when a per-son is incarcerated by military or civilian authorities on conviction of a criminal offense, or when a person is dropped from the rolls as a deserter. In such instances, the commander will take the following actions immediately:

(a) Withdraw the DA Form 873 from the person's MPRJ or OPF and stamp or print across the face, "Revoked by authority of Commander, CCF-- deserted (date)" or "Revoked by authority of Commander, CCF—incarcerated as a result of civil conviction or court-martial (date)," as appropriate for military and civilian personnel. Forward the DA Form 873 and DA Form 5248 explaining the circumstances to the Commander, CCF (PCCF-M).

(b) If the MPRJ or OPF does not contain a DA Form 873, forward DA Form 5248-R, explaining the circumstances, to the Commander, CCF (PCCF-M).

b. An opportunity to reply in writing to such authority as the head of the Component concerned may designate.

(1) The commander will ensure that the person acknowledges receipt of the LOI by signing and dating the form letter enclosed with the LOI. The person will indicate his or her intention of submitting a rebuttal. The form letter will be forwarded immediately to CCF.

(2) The commander will ensure that the person is counseled as to the seriousness of CCF's contemplated action and will offer advice and assistance needed in forming a reply. The person may seek advice from The Judge Advocate General or other lawyer (at his or her own expense) and may request a copy of the investigative files under the provisions of the Privacy Act. Privacy requests must be forwarded to the Chief, Freedom of Information /Privacy Office, U.S. Army Intelligence and Security Command, ATTN: IACSF-FI, Fort George G. Meade, MD 20755-5995. If other than Army investigative records repository files exist, the Freedom of Information (FOI)/Privacy Office will refer the request to the appropriate repository. The individual must provide full name (including aliases), SSN, and date and place of birth. The person's signature must be notarized by a commissioned officer. If the per-son requires an extension of the 60-day suspension, the command security manager should forward a request, with justification, to the Commander, CCF (PCCF-M). An expected completion date will be provided.

(3) The person's response must address each issue raised in CCF's LOI. Any written documentation may be forwarded. Letters of recommendation from supervisory personnel may be attached to the response.
(4) The person will forward the response to CCF through the representative of the commander who provided the LOI. The LOI must be endorsed by at least one commander. The commander should recommend whether the person's clearance should be denied, revoked, or restored. The commander should provide a rationale, addressing the issues outlined in the LOI. Responses to LOIs that do not include the commander's
recommendation will be returned with a request for comments.
c. A written response to any submission under subparagraph b, stating the final reasons therefor, which shall be as specific as privacy and national security considerations permit. The signature authority must be as provided for in paragraphs 6-101b(1)(b) and 6-101b(2)(b). Such response shall be as prompt as individual circumstances permit, not to exceed 60 days from the date of receipt of the appeal submitted under subparagraph b, above, provided no additional investigative action is necessary. If a final response can-not be completed within the timeframe allowed, the subject must be notified in writing of this fact, the reasons therefor, and the date a final response is expected, which shall not, in any case, exceed a total of 90 days from the date of receipt of the appeal under subparagraph b.
(1) CCF's decision is considered final. This decision will be forwarded through the command security office to the individual.
(2) In accordance with AR 600-37 (reference (vv)), CCF must provide unfavorable information developed during the PSI to both the DA Suitability Evaluation Board (DASEB) and the appropriate TAPA, Army Reserve Personnel Center, or Guard Personnel Center personnel management office (PMO) on all senior enlisted (E-6 and above), commissioned, or warrant officer personnel. Specifically included is any information that results in denial or revocation of a security clearance. A copy of CCF's LOI, the person's response, and CCF's final letter will be forwarded. The regulation does not exclude providing other significant unfavorable information that does not in itself result in an adverse decision. The DASEB determines which information is retained in a person's official military personnel file (OMPF). The fact that the information is being forwarded to the DASEB or PMO will be documented in CCF's final letter of determination.
d. An opportunity to appeal to a higher level of authority designated by the Component concerned.
(1) CCF's final letter of determination will state that if the per-son intends to appeal, the appeal must be submitted to HQDA (DAMI-CIS) within 60 days from receipt of the letter. The commander will ensure that the per-son acknowledges receipt of the letter by signing and dating the form letter enclosed with it. If the person does not submit an appeal, the case will be closed, no further appeal will be authorized, and due process will be complete. Requests for extension of time to appeal will be approved only in exceptional cases; they must be in writing, endorsed by the immediate commander, and submitted to HQDA (DAMI-CIS) for approval. Only the subject of the denial or revocation may initiate the appeal. The appeal will be addressed, at a minimum, through the immediate commander. The commander must comment on the action and recommend for or against reinstatement of the security clearance and/or SCI access eligibility. The commander's comments should ad-dress the issues in the CCF LOI. Any appeal will be made solely on the merits as the case stands.
(2) If, upon review of the appeal, a determination by HQDA (DAMI-CIS) results in continued denial or revocation, no further appeal is authorized.

8.201.1 Requests for reconsideration

a. If during the 60 days following receipt of CCF's final letter of determination the subject has additional information in rebuttal or mitigation, he or she should submit it to the Commander, CCF, rather than submitting an appeal to HQDA (DAMI-CIS). DAMI-CIS will forward such information to the CCF Commander. If the CCF review again results in denial or revocation, the person may then appeal to HQDA.
b. If after a final determination by the Commander, CCF, or by HQDA (DAMI-CIS), the person files an appeal, CCF will accept no requests for reconsideration based solely on the passage of time as a mitigating factor for at least 1 year from the date of the final letter of determination or the DA appeal decision, whichever was later.
c. Any request for reconsideration submitted to the Commander, CCF, in accordance with the provisions of subparagraphs a and b, above, must outline the reasons for loss of clearance and provide a rationale for favorable action by CCF. The request for reconsideration must be endorsed by the person's commander. The commander should be familiar

with the information available to CCF and with CCF's rationale for denial or revocation. The commander should state why the clearance and/or SCI access should be restored. If the person is not able to provide the commander with a copy of CCF's original action, the commander should request a copy of the Army Investigative Records Repository dossier through his or her authorized file requester, normally the installation directorate of security (DSEC)/security manager at separate brigade, division, corps, and major command levels.

8.201.2 Involuntary separation of military members and DA civilian personnel

As soon as involuntary separation is considered for military members or DA civilian personnel who have had access to SCI, Special Access programs, or other sensitive programs, the local commander will send the information listed below to HQDA (DAMI-CIS), Washington, DC 20310-1051. Elimination action will not be completed until DAMI-CIS acknowledges receipt of this information.

a. Individual's name, grade, and SSN.
b. Date and place of birth.
c. Marital status.
d. Length of service.
e. Reason(s) for proposed involuntary discharge or dismissal.
f. Type of discharge or dismissal contemplated.
g. Level of access to classified information.

Classified details should not be submitted.

Chapter 9.0 Continuing Security Responsibilities

Section-I Evaluating Continued Security Eligibility
9.100 General

A personnel security determination is an effort to assess the future trustworthiness of an individual in terms of the likelihood of the individual preserving the national security. Obviously it is not possible at a given point to establish with certainty that any human being will remain trustworthy. Accordingly, the issuance of a personnel security clearance or the determination that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action. Rather, there is the clear need to ensure that, after the personnel security determination is reached, the individual's trust-worthiness is a matter of continuing assessment. The responsibility for such assessment must be shared by the organizational commander or manager, the individual's supervisor and, to a large degree, the individual himself. Therefore, the heads of DOD Components shall establish and maintain a program designed to evaluate on a continuing basis the status of personnel under their jurisdiction with respect to security eligibility. This program should en-sure close coordination between security authorities and personnel, medical, legal, and supervisory personnel to ensure that all pertinent information available within a command is considered in the personnel security process.

9.101 Management responsibility

a. Commanders and heads of organizations shall ensure that personnel assigned to sensitive duties (or other duties requiring a trustworthiness determination under the provisions of this regulation) are initially indoctrinated and periodically instructed thereafter on the national security implication of their duties and on their individual responsibilities.
b. The heads of all DOD Components are encouraged to develop programs designed to counsel and assist employees in sensitive positions who are experiencing problems in their personal lives with respect
to such areas as financial, medical or emotional difficulties. Such initiatives should be designed to identify potential problem areas at an early stage so that any assistance rendered by the employing activity will have a reasonable chance of precluding long-term, job-related security problems

9.102 Supervisory responsibility

Security programs shall be established to ensure that supervisory personnel are familiarized with their special responsibilities in matters pertaining to personnel security with respect to personnel under their supervision. Such programs shall provide practical guidance as to indicators that may signal matters of personnel security concern. Specific instructions should be disseminated by security managers concerning reporting procedures to enable the appropriate authority to take timely corrective action to protect the interests of national security as well as to provide any necessary help to the individual concerned to correct any personal problem which may have a bearing upon the individual's continued eligibility for access.
a. In conjunction with the sub-mission of BIs and SBIs stated in chapter 2, section II, and appendix B, paragraphs B-3 and B-4; and with the submission of PRs stated in section VII, chapter3, and para-graph B-5, appendix B; supervisors will be required to review an individual's DD Form 398 to ensure that no significant adverse information of which they are aware and that may have a bearing on subject's initial or continued eligibility for access to classified information is omitted.
b. If the supervisor is not aware of any significant adverse information that may have a bearing on the subject's initial or continued eligibility for access, then the following statement must be documented, signed and dated, and forwarded to DIS with the investigative package. "I am aware of no information of the type contained at appendix E, DOD 5200.2-R, (AR 380-67) relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely

on his/her ability to safeguard classified information."
c. If the supervisor is aware of such significant adverse information, the following statement shall be documented, signed and dated, and for-warded to DIS with the investigative package, and a written summary of the derogatory information forwarded to DIS with the investigative package: "I am aware of in-formation of the type contained in appendix E, DOD5200.2-R (AR 380-67), relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information and have reported all relevant details to the appropriate security official(s)." d. In conjunction with regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information, supervisors will include a comment in accordance with paragraphs 9-102b and c, above, as well as a comment regarding an employee's discharge of security responsibilities, pursuant to their Component guidance.
e. If the statement in paragraph 9-102c, above applies, the supervisor must ensure that all relevant information is reported to the local command security official responsible for processing the investigative paperwork.
f. If the information seems to warrant adverse action, the command security official will immediately refer it to the Commander, CCF (PCCF-M), using DA Form 5248-R. CCF will process the cases in accordance with established procedures.
g. If the local command security official determines that the information is minor and does not war-rant an adverse action, the PSI request should be forwarded to DIS. A summary of the derogatory information will be part of the investigative request packet. DIS will initiate the investigation and expand as appropriate. DIS will forward results of the investigation to CCF for adjudication.
h. It is important that immediate supervisors take an objective approach to the requirements in b and c, above, to ensure equity to both the subject of the investigation and national security.

9.103 Individual responsibility

a. Individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding positions of trust. In this connection, individuals must recognize and avoid the kind of personal behavior that would result in rendering one ineligible for continued assignment in a position of trust. In the final analysis, the ultimate responsibility for maintaining continued eligibility for a position of trust rests with the individual.
b. Moreover, individuals having access to classified information must report promptly to their security office:
(1) Any form of contact, intentional or otherwise, with a citizen of a designated country, (app H) unless occurring as a function of one's official duties.
(2) Attempts by representatives or citizens of designated countries to cultivate friendships or to place one under obligation.
(3) Attempts by representatives or citizens of foreign countries to:
(a) Cultivate a friendship to the extent of placing one under obligation that they would not normally be able to reciprocate, or by offering money payments or bribery to obtain information of actual or potential intelligence value.
(b) Obtain information of actual or potential intelligence value through observation, collection of documents, or by personal contact.
(c) Coerce by blackmail, by threats against or promises of assistance to relatives living under foreign control, especially those living in a designated country.
(4) All personal foreign travel in advance.
(5) Any information of the type referred to in paragraph 2-200 or appendix I.

9.104 Coworker responsibility

Coworkers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

Section II Security Education
9.200 General

The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them. Thus, an integral part of the DOD security program is the indoctrination of individuals on their security responsibilities. Moreover, such indoctrination is essential to the efficient functioning of the DOD personnel security pro-gram. Accordingly, heads of DOD Components shall establish procedures in accordance with this chapter whereby persons requiring access to classified information, or being assigned to positions that require the occupants to be determined trustworthy are periodically briefed as to their security responsibilities.

9.201 Initial briefing

a. All persons cleared for access to classified information or assigned to duties requiring a trustworthiness determination under this regulation shall be given an initial security briefing. A record of this briefing will be maintained in the security office. The briefing shall be in accordance with the requirements of paragraph 10-102, DOD5200.1-R (AR 380-5) (reference (q)) and consist of the following elements:
(1) The specific security requirements of their particular job.
(2) The techniques employed by foreign intelligence activities in

attempting to obtain classified information and their responsibility for reporting such attempts (AR381-12) (reference (rr)).
(3) The prohibition against disclosing classified information, by any means, to unauthorized persons or discussing or handling classified information in a manner that would make it accessible to unauthorized persons.
(4) The penalties that may be imposed for security violations.
b. If an individual declines to exe-cute Standard Form189, "Classified Information Nondisclosure Agreement," the DOD Component shall initiate action to deny or revoke the security clearance of such person in accordance with paragraph 8-201 above.

9.202 Refresher briefing

Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in paragraph 10-101, DOD5200.1-R (AR380-5) (reference (q)) shall be tailored to fit the needs of experienced personnel.

10.100 General

In recognition of the sensitivity of personnel security reports and records, particularly with regard to individual privacy, it is Department of Defense policy that such personal information shall be handled with the highest degree of discretion. Access to such information shall be afforded only for the purpose cited herein and to persons whose official duties require such information. Personnel security investigative reports may be used only for the purposes of determining eligibility of DOD military and civilian personnel, contractor employees, and other persons affiliated with the Department of Defense, for access to classified information, assignment or retention in sensitive duties or other specifically designated duties requiring such investigation, or for law enforcement and counter- intelligence investigations. Other uses are subject to the specific written authorization of the Deputy Under Secretary of Defense for Policy.

Table H-1 List of designated countries (located on page 46, AR 380-67)

Country or area	*Approximate control date*	*Country or area*	*Approximate control date*
Afghanistan	April 1978	Kurile Islands/Sakhalin	September 1945
Albania	January 1946	Laos	June 1977
Angola	November 1975	Latvia	June 1940
Berlin (Soviet Sector)	April 1946	Libyan Arab Republic	September 1969
Bulgaria	October 1946	Lithuania	June 1940
Cambodia (Kampuchea)	April 1975	Mongolia, Outer (MPR)	July 1979
China (includes Tibet)	October 1949	Nicaragua	July 1979
Cuba	December 1960	Poland	February 1947
Czechoslovakia	February 1948	Rumania	December 1947
Estonia	June 1940	Southern Yemen	June 1969
Ethiopia	September 1974	Syria	February 1958
Germany, East (GDR)	April 1946	USSR	October 1922
Hungary (HPR)	June 1947	Vietnam, North (DRV)	December 1946
Iran	February 1978	Vietnam, South	April 1975
Iraq	July 1958	Yugoslavia	November 1945
Korea, North (DPRK)	September 1945		

End of AR 380-67 Extract.

Student Handout 3

Extract

Pages SH-3-2 and SH-3-3 of this student handout are an extract from AR 380-5, Department of the Army Information Security Program, 29 September 2000.

(EXTRACT)

Security

Department of the Army Information Security Program

Headquarters
Department of the Army
Washington, DC
29 September 2000

UNCLASSIFIED

have confidence in the sharing of information with other agencies, the national, DOD, and DA policy, contained in

this regulation, will be followed.
b. Unless otherwise noted, requests for waivers to the requirements contained in this regulation, will be submitted, through command channels, to DAMI-CH. Waivers to DOD requirements will be forwarded by DAMI-CH, for decision to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C31)). For requirements related to Two-Person Integrity (TPI), RD, Foreign Government Information (FGI) (including North Atlantic Treaty Organization (NATO)), and security arrangements for international programs, waivers will be forwarded to the Under Secretary of Defense (Policy)(USD(P)). Waivers for SAPs will be submitted, through SAPs channels, to DAMI-CH for coordination with TMO and, as required, forwarded to the Under Secretary of Defense (Special Programs) (USD(SP)). The ASD(C31) and USD(P) are responsible for notifying the Director of the ISOO of the waivers approved that involve EO 12958 and its implementing directives.
c. Before submitting a request for waiver, the requesting authority will consider risk management factors such as criticality, sensitivity, and value of the information, analysis of the threats both known and anticipated, vulnerability to exploitation, and countermeasure benefits versus cost (national security cost and resource cost). Requests for waiver must contain sufficient information to permit a complete and thorough analysis to be made of the impact on national security if the waiver is approved. The waiver request will also describe all the factors creating the special situation and the alternative or compensatory measures which make sure the protection afforded the information is sufficient to reasonably deter and detect loss or unauthorized disclosure. The requesting command will maintain documentation regarding approved waivers, including the alternative or compensatory measures approved and in use, and furnish this documentation, upon request, to other agencies and to other Army commands, with whom classified information or secure facilities are shared.
Note: Waivers granted before the effective date of this regulation are canceled no later than one year after the effective date of this regulation. New/updated waiver requests may be submitted prior to cancellation date.
d. Throughout this regulation there are references to policy subject to MACOM approval or subject to policy as the MACOM directs. Where that language, in substance, is used, the MACOM commander, or the HQDA SAAA, for cases involving HQDA and its Field Operating Agencies (FOA), can delegate such approval authority. The delegations will be in writing. A copy of such delegations will be maintained by the appointing official and reviewed periodically for review of need for continuation. Where this regulation specifically specifies waiver authority to a MACOM commander or the HQDA SAAA, that authority resides solely with the MACOM commander or HQDA SAAA and will not be further delegated.

Section VII
Corrective Actions and Sanctions

1-20. General
Commanders will establish procedures to make sure that prompt and appropriate action is taken concerning a violation of the provisions of this regulation, especially in those cases involving incidents which can put classified information at risk of compromise, unauthorized disclosure, or improper classification of information. Such actions will focus on a correction or elimination of the conditions that caused or contributed to the incident.

1-21. Sanctions
a. DA personnel will be subject to sanctions if they knowingly, willfully, or negligently—
(1) Disclose classified or sensitive information to unauthorized persons.
(2) Classify or continue the classification of information in violation of this regulation.
(3) Violate any other provision of this regulation.
b. Sanctions can include, but are not limited to warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of original classification authority. Action can also be taken under the Uniform Code of Military Justice (UCMJ) for violations of that Code and under applicable criminal law, if warranted.
c. Original classification authority will be withdrawn for individuals who demonstrate a disregard or pattern of error in applying the classification and sensitivity standards of this regulation.

1-22. Reporting of Incidents
EO 12958, paragraph *5.7(e)(2),* requires that the director of the ISOO be advised of instances in which classified information is knowingly, willfully, or negligently disclosed to unauthorized persons, or instances of classifying, or continuing the classification of, information in violation of this regulation. Reports of those instances will be submitted through command channels to DAMI-CH for forwarding to the director of the ISOO and other defense officials as appropriate. See chapter 10 for reporting of other security incidents.